PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of

Jens-Peter REDLICH, et al.

Appln. No.: 10/057,914

Confirmation No.: 3714

Filed: January 29, 2002

Docket No: A7995

Group Art Unit: 2141

Examiner: Chirag R. PATEL

For: MULTI-ISP CONTROLLED PUBLIC INTERNET ACCESS, BASED ON THIRD-PARTY OPERATED PUBLIC ACCESS STATIONS

SUBMISSION OF APPEAL BRIEF

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The statutory fee of $500.00 is being charged to Deposit Account No. 19-4880 via EFS Payment Screen. The USPTO is also directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

Chid S. Iyer
Registration No. 43,355

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: May 18, 2007

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of	Docket No: A7995
Jens-Peter REDLICH, et al.	
Appln. No.: 10/057,914	Group Art Unit: 2141
Confirmation No.: 3714	Examiner: Chirag R. PATEL
Filed: January 29, 2002	

For: MULTI-ISP CONTROLLED PUBLIC INTERNET ACCESS, BASED ON THIRD-PARTY OPERATED PUBLIC ACCESS STATIONS

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 41.37, Appellant submits the following:

Table of Contents

I. REAL PARTY IN INTEREST

The real party in interest is NEC USA, INC. (Assignee) by virtue of an assignment executed by the inventors Jens-Peter REDLICH, Thomas KUEHNEL and Wolf MUELLER on February 20, 2002, February 28, 2002 and March 9, 2002, respectively and filed on March 15, 2002 along with form PTO-1595.

II. RELATED APPEALS AND INTERFERENCES

Upon information and belief, there are no other prior or pending appeals, interferences, or judicial proceedings known to Appellants, Appellants' representatives or the Assignee that may be related to, be directly affected by, or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

Each of the pending claims 1-41 are rejected (see Final Office Action dated November 22, 2006).

IV. STATUS OF AMENDMENTS

There are no pending unentered amendments.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Appellants invention relates to techniques for providing secure public access to an IP network using third-party operated access stations in a situation where the access station is an "untrusted" access station. Using these techniques authentication, authorization, accounting, and ciphering of data for access to an IP network can be done via access stations that are operated by potentially malicious and untrusted third-parties.

Nowadays, small independent operators offer Internet access in a small geographical area. For example, users can access content providers on the Internet using their own devices (PDAs or laptops) sitting in coffee shops (for example, Starbucks). Such an access to the Internet uses access stations provided by the independent operator. However, trustworthiness of the independent is not guaranteed. Malicious operators may find it easy to eavesdrop on the communication between the user and the content provider. They might also find means to obtain credentials like login names and passwords from the user's traffic. The present invention provides secure access that is independent of such an operator's access station.

The exemplary embodiment of depicted in FIG. 1 shows a secure tunnel (1) that is established between a terminal user U (3) and trusted node T (5) via access station A (7). The user U seeks authentication from the ISP (4). Once terminal U (3) and ISP P (4) are authenticated, ISP P selects a trusted node T (5). The ISP P (4) distributes session keys to terminal U (3) and trusted node (5). **Importantly, this secret session key is not known to the access station A.** All further communication between U and T is performed by encrypting the data using the secret session key. Thus a secure tunnel (1) between U and T is established. Using

the secure tunnel (1), terminal U (3) transmit encrypted data packets to trusted node T (5).

FIG. 2 shows an example of the authentication and session key transfer between terminal U (3), access station A (7), ISP P (4) and trusted node T (5). Specifically authentication procedures are performed between terminal U (3) and ISP P (4) via access station A (7). Upon the valid authentication of both terminal U (3) and ISP P (4), ISP P (4) generates and distributes session keys to a trusted node T (5) and terminal U (3) as depicted by the short dash line. As noted above, all subsequent data between terminal U (3) and trusted node T (5) are encrypted and sent via the secure tunnel (1) which passes through access station A (7). Since the encryption is done based on the secret session key unknown to the access station A, it cannot decipher or modify the data packet. In other words, access station A (7) is forced to simply acts as a conduit between terminal U (3) and trusted node T (5) while trusted node T (5) forwards and receives data packets from the IP network (9).

The present invention, as recited in claim 1, provides a method for performing mutual authentication and authorization of a user's terminal device (U) and an Internet Service Provider (P) in order to establish secure communication between the terminal (U) and a trusted network element (T) to the Internet via an untrusted access station (A) (Specification [0012]). An association is established between a terminal (U) and an untrusted access station (A) (Specification [0063] ll.4-6). An ISP authentication packet is transmitted from terminal (U) to ISP (P) via the untrusted access station (A) (Specification [0068]-[0078]). A user authentication packet is sent from said ISP (P) to said terminal (U) via said untrusted access station (A)

(Specification [0082]-[0090]). Upon authentication of said terminal (U) and said ISP (P), said ISP generates a session key and distributing the session key to said terminal (U) and a trusted network element (T) (Specification [0097]). The session key is used to encrypt traffic between the terminal (U) and the trusted network element (T) (Specification [0097]). Thus a secure tunnel is established such that the terminal (U) may communicate with the Internet via said trusted network element (T) (Specification [0097]). The secure tunnel emulates a physical link between the terminal (U) and the trusted network element (T) such that traffic transmitted between the terminal (U) and said Internet via said trusted network element (T) is secure from modification or eavesdropping by said untrusted access station (A) (Specification [0108]). A connection is established between the terminal and the ISP for trusted network services without providing the terminal with direct access to the Internet (Specification [0107]-[0110]).

The present invention, as recited in claim 4, is a method for providing public access to IP-based networks via an untrusted infrastructure having untrusted access points. A connection is established between an IP-device (U) and said untrusted access point (A), wherein an IP address is dynamically allocated to the IP device (Specification [0063]). An ISP authentication request is transmitted from said IP device (U) to an internet service provider (P) affiliated with said IP device (U) (Specification [0068]-[0078]). The authentication request is transmitted through said untrusted access point (A) affiliated with said untrusted third party owned infrastructure (Specification [0068]-[0078]). A user authentication request is transmitted from the ISP (P) to the IP device (U) to determine whether the IP device (U) is a valid user affiliated with said ISP

(P), wherein said authentication request is transmitted through said untrusted access point (A) affiliated with said untrusted third party owned infrastructure (Specification [0079]-[0087]).When said ISP (P) authentication request and said user authentication requests is affirmative, the ISP (P) generates a key session for encrypting data packets and distributes said session key to said IP device (U) and a trusted node (T) (Specification [0097]). The session key is used to encrypt data transmitted between said IP device (U) and said trusted node (T). (Specification [0097]) Thus a secure tunnel is established as said session key is used to encrypt data packets transmitted between said IP device (U) and said trusted node (T), such that said data packets transmitted between said IP device (U) and an Internet via the untrusted access station (A) are protected from modification and manipulation by said untrusted access station (A) in said secure tunnel (Specification [0108]). The connection is established between the terminal and the ISP for trusted network services without providing the terminal with direct access to the Internet (Specification [0107]-[0110]).

The present invention, as recited in claim 5 is a method for providing public access to IP-based networks through a third party owned, untrusted infrastructure having untrusted access stations ((Specificaiton [0012]). A connection is established between an IP-device (U) and said access station (A) wherein an IP address is dynamically allocated to said IP device (U) (Specificaiton [0063]). An ISP authentication request is sent to said internet service provider (P) affiliated with said IP device (U) requesting to validate the authenticity of the ISP (P) (Specificaiton [0068]-[0078]). A user authentication request is sent from said ISP (P) to said IP

device (U) to validate whether said IP device (U) has a service agreement with said ISP (P) (Specificaiton [0079]-[0087). On affirmative authentication of said ISP (P) and said IP device (U), a trusted connection is established between said IP device (U) and a trusted network element (T) (Specificaiton [0097]). The secure tunnel allows the ISP (P) to dynamically obtain control of resource in said untrusted third party owned access station (A) in order to provide the IP device (U) with prescribed for services (Specificaiton [0011]). The connection is established between the terminal and the ISP for trusted network services without providing the terminal with direct access to the Internet (Specificaiton [0107]-[0110]).

The present invention, as recited in claim 6, is method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over a third party owned untrusted access station (A) (Specificaiton [0012]). A connection is established between the terminal (U) and said access station (A) (Specificaiton [0063]). An ISP authentication request is sent to said internet service provider (P) affiliated with said terminal (U) (Specificaiton [0068]- [0078]). A user authentication request is sent from said ISP (P) to said terminal (U) (Specificaiton [0079]-[0087]). On affirmative authentication of said ISP (P) and said terminal (U) a trusted connection is established between said IP device (U) and a trusted network element (T) (Specification [0097]). A secure tunnel allows the ISP (P) to dynamically obtain control of resource in said untrusted access station (A) in order to provide the IP device (U) with prescribed for services (Specifcation [0011]). The

connection is established between the terminal and the ISP for trusted network services without providing the terminal with direct access to the Internet (Specificaiton [0107]-[0110]).

The present invention, as recited in claim 35, is a computer program product having software instructions for enabling the computer to perform some of the operations described above.

The present invention, as recited in claim 36, is a method of operating an untrusted access station deployed so as to provide a local network with access to a wide area network, the method comprising. A untrusted access station receives a request from a terminal to access trusted network services (Specification [0063]). Without providing the terminal with direct access to the wide area network, establishing a connection between the terminal and an authentication server for trusted network services (Specification [0063]-[0067]). Authentication of the terminal with the authentication server for the trusted network services is performed (Specification [0072]-[0079]). The terminal is allowed to establish a secure channel to trusted network services across the wide area network only if the authentication succeeds (Specification [0097]).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Rejection of claims 1-22, 24-25, 28, 30, 33, 35-37 and 39-41 under 35 U.S.C. 102(e) as being anticipated by Giniger et al (U.S. Patent No. 6,751,729).

2. Rejection of claims 23, 26-27, 29, 31-32, 34 and 38 under 35 U.S.C. 103(a) as being unpatentable over Giniger et al. (U.S. Patent No. 6,751,729) in view of Rueda et a. (U.S. Publication No. 2002/0112076).

VII. ARGUMENT

1. Claims 1-22, 24-25, 28, 30, 33, 35-37 and 39-41 are not anticipated by Giniger

Giniger merely discloses a conventional virtual private network setup. The virtual network is established between a plurality of "edge devices." (Giniger 7:36-40). The edge device acts as an intermediary between a local network of computers and the VPN. Thus, a packet from a user computer device would travel through the local network, arrive at the edge device, and the edge device would intelligently decide which VPN tunnel to send it through so as to arrive its destination (Giniger 7:54-64). The edge devices include cryptographic modules so as to ensure that the tunnels established between the edge devices are secure (Giniger 10:37-54). **In other words all the cryptographic function including encryption is performed at the edge device**. Therefore, the edge device **must be trusted** to include the cryptographic module and establish the secure tunnels. Thus, in Giniger, specific manufacturing rules for ensuring that the cryptographic certificates are stored in a tamper-resistent portion of the edge device are provided (Giniger 12:50-59).

The present invention relates to methods for performing mutual authentication and authorization of a users terminal and an ISP to provide a secure communication between the terminal and a trusted element to the internet via an **untrusted access station.** For example, in the embodiments shown on Figs. 1 and 2, the user terminal 3 is connected to the trusted network element 5 via an untrusted access station 4. The sequence of steps are described in relation to Figs. 1 and 2.

The exemplary embodiment of depicted in FIG. 1 shows a secure tunnel (1) that is established between a terminal user U (3) and trusted node T (5) via access station A (7). The user U seeks authentication from the ISP (4). Once terminal U (3) and ISP P (4) are authenticated, ISP P selects a trusted node T (5). The ISP P (4) distributes session keys to terminal U (3) and trusted node (5). **Importantly, this secret session key is not known to the access station A.** All further communication between U and T is performed by encrypting the data using the secret session key. Thus a secure tunnel (1) between U and T is established. Using the secure tunnel (1), terminal U (3) transmit encrypted data packets to trusted node T (5).

FIG. 2 shows an example of the authentication and session key transfer between terminal U (3), access station A (7), ISP P (4) and trusted node T (5). Specifically authentication procedures are performed between terminal U (3) and ISP P (4) via access station A (7). Upon the valid authentication of both terminal U (3) and ISP P (4), ISP P (4) generates and distributes session keys to a trusted node T (5) and terminal U (3) as depicted by the short dash line. As noted above, all subsequent data between terminal U (3) and trusted node T (5) are encrypted and sent via the secure tunnel (1) which passes through access station A (7). Since the encryption is done based on the secret session key unknown to the access station A, it cannot decipher or modify the data packet. In other words, access station A (7) is forced to simply acts as a conduit between terminal U (3) and trusted node T (5) while trusted node T (5) forwards and receives data packets from the IP network (9).

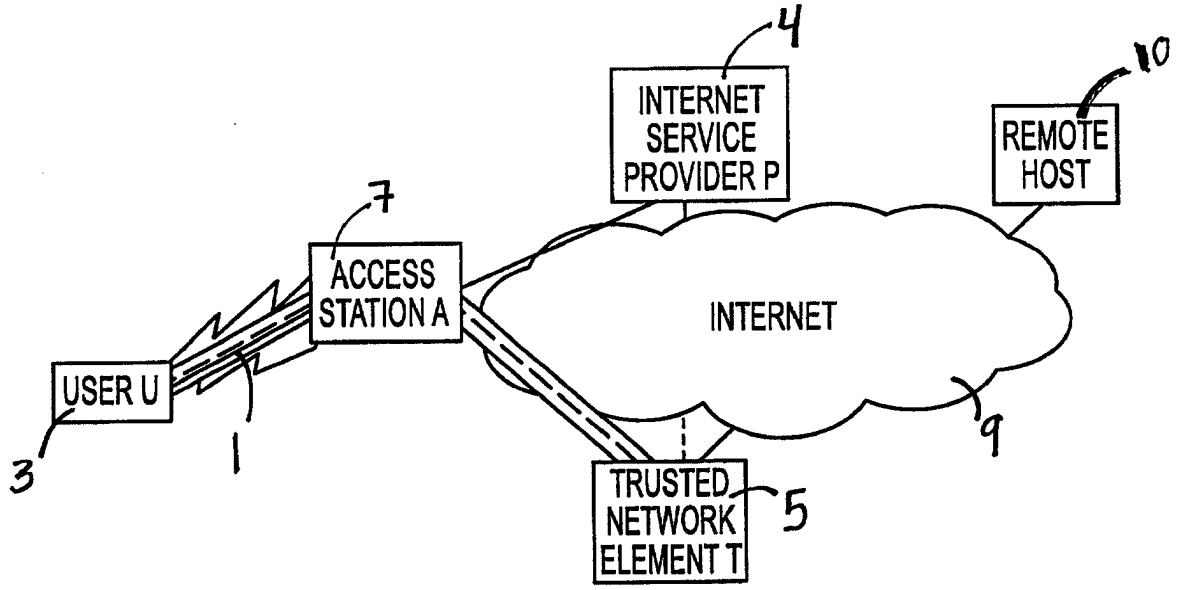

4
INTERNET SERVICE PROVIDER P
10
REMOTE HOST
7
ACCESS STATION A
INTERNET
USER U
3
1
9
TRUSTED NETWORK ELEMENT T
5

FIG. 1

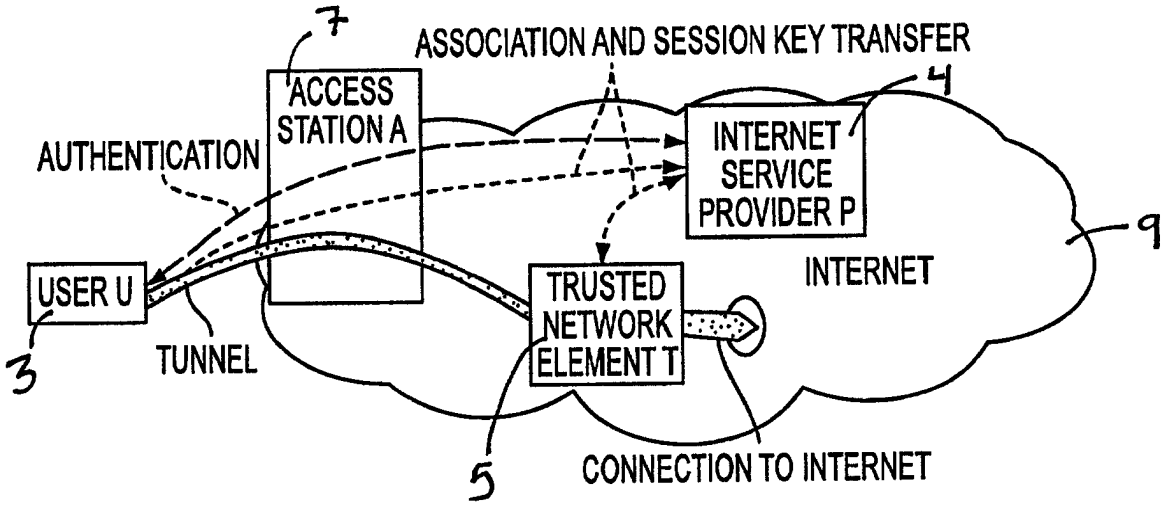

7
ASSOCIATION AND SESSION KEY TRANSFER
ACCESS STATION A
4
AUTHENTICATION
INTERNET SERVICE PROVIDER P
9
INTERNET
USER U
TRUSTED NETWORK ELEMENT T
3
TUNNEL
5
CONNECTION TO INTERNET

FIG. 2

The extensive prosecution of this case will reveal that a key point of difference between the Examiner's position and the Appellants position is regarding whether the end node of Giniger can be considered to be "untrusted."

Giniger includes a general teaching on providing secure service communication services over a data network. Further, it teaches establishing a tunneling communication service. However, the specific issue of accessing an internet in a trusted way between a user terminal via an **untrusted access station** is not even remotely suggested. The end node of Giniger cannot be considered to be an untrusted access station as in the present invention. Notably, the end node of Giniger is actively involved in authentication, encryption ,etc. In fact. since the edge device is actively involved in providing a secure tunnel, the device of Giniger should expect that the edge device is trusted, unlike in the present invention.

Specifically, the present invention (as recited in claim 1) requires establishing an association between a terminal and an **untrusted access station**. Giniger does not disclose or suggest establishing such an association between a terminal and an **untrusted access station**.

Further, the present invention requires distributing a secure key to a trusted network element for encrypting traffic between the terminal and the trusted network element. Using the encryption, a secure tunnel is established such that the terminal may communicate with the internet via the trusted network element. Specifically, the secure tunnel is required to be established in such a way that the traffic in the secure tunnel is secure from modification by the

access station. On the other hand, in Giniger since the edge device is involved in encryption, it can easily modify or maliciously interfere with the data.

The passages cited by the Examiner (15:19-22) merely suggests establishing tunnels between edge nodes.

The Final Office Action dated July 13, 2005, is the only instance of the Examiner attempting to counter the Applicant's arguments that the edge device of Giniger is not an "untrusted" access station required by the present invention. On page 4 of this Office Action, referring to 6:14-22 of Giniger, the Examiner simply notes that Giniger provides comprehensive security for exchanging information. However, the Examiner has not provided any reason for why he construes the edge device of Giniger to be an untrusted access station.

The present invention relates to techniques for providing a secure communication channel between a user terminal and a trusted network element via an untrusted access station. Giniger des not disclose (or suggest) such a technique.

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." MPEP 2131 *citing Verdegaal Bros. v. Union Oil Co. of California,* 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

The Examiner has not established anticipation of the present invention (as recited in claim 1) by Giniger at least because Giniger does not disclose establishing a secure tunnel

between a user terminal and a trusted network element via an untrusted access station. Therefore, finding of anticipation of claim 1 by Giniger must be reversed.

Claims 4, 5, 6 and 36 include features that are discussed above that are analogous to claim 1 (specifically the limitations related to "untrusted" access station). Therefore, the rejection of these claims under section 102 (b) based on Giniger must also be reversed.

Claims 2, 3, 7-21, 24-25, 28, 30 and 30 are dependant on claims 1 and 6, respectively. Therefore, they are patentable for the same reasons.

Claim 35 recites a computer program product and includes limitations analogous to the ones discussed above. Therefore, it is patentable at least for analogous reasons.

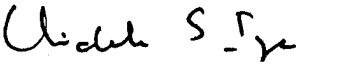
Claims 23, 26-27, 29, 31-32 and 34 are not obvious over Giniger and Rueda

The above claims are dependant on claim 6, and therefore, are allowable for at least the same reasons. Further, Rueda does not overcome the deficiencies noted above in the teachings of Giniger. Therefore, the finding of obviousness based on the combined teachings of Giniger and Rueda must also be reversed.

Unless a check is submitted herewith for the fee required under 37 C.F.R. §41.37(a) and 1.17(c), please charge said fee to Deposit Account No. 19-4880.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,



Chid S. Iyer
Registration No. 43,355

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: May 18, 2007

CLAIMS APPENDIX

CLAIMS 1-41 ON APPEAL:

1. (previously presented): A method for performing mutual authentication and authorization of a user's terminal device (U) and an Internet Service Provider (P) in order to establish secure communication between the terminal (U) and a trusted network element (T) to the Internet via an untrusted access station (A) comprising:

establishing an association between a terminal (U) and an untrusted access station (A);

transmitting an ISP authentication packet from terminal (U) to ISP (P) via the untrusted access station (A);

sending a user authentication packet from said ISP (P) to said terminal (U) via said untrusted access station (A);

upon authentication of said terminal (U) and said ISP (P), said ISP performs the following:

generating a session key;

distributing said session key to said terminal (U) and a trusted network element (T), wherein said session key is used to encrypt traffic between the terminal (U) and the trusted network element (T);

establishing a secure tunnel such that the terminal (U) may communicate with the Internet via said trusted network element (T);

wherein said secure tunnel emulates a physical link between the terminal (U) and the trusted network element (T) such that traffic transmitted between the terminal (U) and said Internet via said trusted network element (T) is secure from modification or eavesdropping by said untrusted access station (A),

wherein a connection is established between the terminal and the ISP for trusted network services without providing the terminal with direct access to the Internet.

2. (previously presented): The method for performing mutual authentication and authorization of a terminal (U) and an Internet Service Provider (P) in order to establish a secure tunnel between the terminal (U) and a trusted network element to the Internet (T) via an untrusted access station (A) of claim 1, wherein the ISP (P) authentication packet contains an authentication challenge (CH_U) from terminal (U) to ISP (P) to authenticate the identity of ISP (P).

3. (previously presented): The method for performing mutual authentication and authorization of a terminal (U) and an Internet Service Provider (P) in order to establish a secure tunnel between the terminal (U) and a trusted network element to the Internet (T) via an untrusted access station (A) of claim 1, wherein the user authentication packet contains an authentication challenge (CH_P) from ISP (P) to the terminal (U) to authenticate the identity of user (U).

4. (previously presented): A method for providing public access to IP-based networks via an untrusted infrastructure having untrusted access points comprising:

establishing a connection between an IP-device (U) and said untrusted access point (A), wherein an IP address is dynamically allocated to said IP device;

transmitting an ISP authentication request from said IP device (U) to an internet service provider (P) affiliated with said IP device (U), wherein said authentication request is transmitted through said untrusted access point (A) affiliated with said untrusted third party owned infrastructure;

transmitting a user authentication request from said ISP (P) to said IP device (U) to determine whether said IP device (U) is a valid user affiliated with said ISP (P), wherein said authentication request is transmitted through said untrusted access point (A) affiliated with said untrusted third party owned infrastructure;

when said ISP (P) authentication request and said user authentication requests is affirmative, said ISP (P):

generates a key session for encrypting data packets; and

distributes said session key to said IP device (U) and a trusted node (T), wherein said session key is used to encrypt data transmitted between said IP device (U) and said trusted node (T);

establishing a secure tunnel as said session key is used to encrypt data packets transmitted between said IP device (U) and said trusted node (T), such that said data packets transmitted

between said IP device (U) and an Internet via the untrusted access station (A) are protected from modification and manipulation by said untrusted access station (A) in said secure tunnel,

wherein a connection is established between the terminal and the ISP for trusted network services without providing the terminal with direct access to the Internet.

5. (previously presented): A method for providing public access to IP-based networks through a third party owned, untrusted infrastructure having untrusted access stations (A) comprising:

establishing a connection between an IP-device (U) and said access station (A), wherein an IP address is dynamically allocated to said IP device (U);

sending an ISP authentication request to said internet service provider (P) affiliated with said IP device (U) requesting to validate the authenticity of the ISP (P);

sending a user authentication request from said ISP (P) to said IP device (U) to validate whether said IP device (U) has a service agreement with said ISP (P);

upon affirmative authentication of said ISP (P) and said IP device (U);

establishing a trusted connection between said IP device (U) and a trusted network element (T), wherein a secure tunnel allows the ISP (P) to dynamically obtain control of resource in said untrusted third party owned access station (A) in order to provide the IP device (U) with prescribed for services,

wherein a connection is established between the terminal and the ISP for trusted network services without providing the terminal with direct access to the Internet.

6. (previously presented): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over a third party owned untrusted access station (A) comprising:

establishing a connection between the terminal (U) and said access station (A);

sending an ISP authentication request to said internet service provider (P) affiliated with said terminal (U);

sending a user authentication request from said ISP (P) to said terminal (U);

upon affirmative authentication of said ISP (P) and said terminal (U):

establishing a trusted connection between said IP device (U) and a trusted network element (T), wherein a secure tunnel allows the ISP (P) to dynamically obtain control of resource in said untrusted access station (A) in order to provide the IP device (U) with prescribed for services,

wherein a connection is established between the terminal and the ISP for trusted network services without providing the terminal with direct access to the Internet.

7. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the ISP authentication request contains an authentication challenge (CH_U) from terminal (U) to ISP (P) to authenticate the identity of ISP (P).

8. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the user authentication request contains an authentication challenge (CH_P) from ISP (P) to the terminal (U) to authenticate the identity of terminal (U) as having subscribed to said ISP (P) for services.

9. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, the ISP (P) generates a session key for encrypting data packets upon the affirmative authentication of the terminal (U) and the ISP (P).

10. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the ISP (P) selects a trusted node (T) with said Internet.

11. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 9, wherein said ISP (P) distributes said session key to the terminal (U) and the trusted node (T).

12. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the session key is used to encrypt data packets transmitted between the terminal (U) and the trusted node (T).

13. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 12, wherein the transmission of encrypted data packets between the terminal (U) and the trusted node (T) established a secure tunnel.

14. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 13, wherein the secure tunnel protects the data packets from manipulation by said untrusted access station (A).

15. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, a time out is distributed to the trusted node (T) and terminal (U) upon the establishment of a secure tunnel.

16. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 15, wherein the timeout value is set to a predetermined time period, wherein if the secure tunnel is active for a time period equal to the timeout value, the secure tunnel will expire and the resources utilized for the secure tunnel will be releases.

17. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein upon receipt of an encrypted data packet from the terminal (U), the trusted node (T) decrypts the data packet and forwards the decrypted data packet to the Internet.

18. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 17, wherein upon receipt of an encrypted data packet from the terminal (U), the trusted node (T) decrypts the data packet and forwards the decrypted data packet to a remote communication peer (R).

19. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 18, wherein the Internet sends an original data packet to the terminal (U) via the trusted node (T), wherein the trusted node (T) encrypts the original data packet and forwards the encrypted data packet to the terminal (U) via the untrusted access station (A).

20. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 17, wherein upon receipt of the encrypted data packet from the trusted node (T), the terminal (U) utilizes the session key to decrypt the data packet thus yielding the original data packet from the Internet.

21. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 18, wherein a remote communication peer (R) sends an original data

packet to the terminal (U) via the trusted node (T), wherein the trusted node (T) encrypts the original data packet and forwards the encrypted data packet to the terminal (U) via the untrusted access station (A).

22. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 21, wherein upon receipt of the encrypted data packet from the trusted node (T), the terminal (U) utilizes the session key to decrypt the data packet thus yielding the original data packet from the remote communication peer (R).

23. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the ISP (P) provides an accounting of time to the untrusted access station (A) for resources utilized by the terminal (U).

24. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the untrusted access station (A) is incorporated into a third party owned network infrastructure.

25. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 24, wherein the ISP (P) provides the terminal (U) with at least one subscribed for service via an untrusted access station (A).

26. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the ISP (P) reimburses the untrusted access station (A) for resources expended on the terminal (U) according to an accounting of time.

27. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 25, wherein the ISP (P) bills the terminal (U) for services provided to the terminal (U).

28. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 24, wherein the untrusted access station (A) is located in the network infrastructure of a public facility.

29. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 28, wherein the public facility is at least one of an airport, a convention center, a restaurant, a hotel, a library, and a school.

30. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 24, wherein the untrusted access station (A) is located within the infrastructure of a private household or within the private infrastructure of a corporation or government institution.

31. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the untrusted access stations (A) is compatible with at least one wireless transmission standard including WLAN (IEEE 802.11), BlueTooth (IEEE 802.15), or HiperLan.

32. (previously presented): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the terminal (U) is a mobile device.

33. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the terminal (U) recognizes a compatible access point by broadcasting a dynamic host configuration protocol (DHCP) request and receiving a "magic" DHCP response from the untrusted access station (A).

34. (original): A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the untrusted access station (A) assigns an local unique identification (LUID) to the terminal (U) in order to facilitate matching the terminal with data packets when the untrusted access station (A) is simultaneously serving multiple terminals (U).

35. (previously presented): A computer program product for accessing and authenticating Internet service via an untrusted access point comprising:

software instructions for enabling the computer to perform predetermined operations, and

a computer readable medium bearing the software instructions;

the predetermined operations including

establishing a connection between an IP-device (U) and said access station (A), wherein an IP address is dynamically allocated to said IP device (U);

sending an ISP authentication request to said internet service provider (P) affiliated with said IP device (U) requesting to validate the authenticity of the ISP (P);

sending a user authentication request from said ISP (P) to said IP device (U) to validate whether said IP device (U) has a service agreement with said ISP (P);

upon affirmative authentication of said ISP (P) and said IP device (U).

establishing a trusted connection between said IP device (U) and a trusted network element (T), wherein a secure tunnel allows the ISP (P) to dynamically obtain control of resource

in said untrusted third party owned access station (A) in order to provide the IP device (U) with prescribed for services,

wherein a connection is established between the terminal and the ISP for trusted network services without providing the terminal with direct access to the Internet.

36. (previously presented): A method of operating an untrusted access station deployed so as to provide a local network with access to a wide area network, the method comprising:

an untrusted access station receiving a request from a terminal to access trusted network services;

without providing the terminal with direct access to the wide area network, establishing a connection between the terminal and an authentication

server for trusted network services

performing authentication of the terminal with the authentication server for the trusted network services;

allowing the terminal to establish a secure channel to

trusted network services across the wide area network only if the authentication succeeds.

37. (previously presented) The method of claim 36 wherein the authentication is performed using messages protected by public key cryptography.

38. (previously presented): The method of claim 36 further comprising charging operators of the trusted network services for usage of the untrusted access station.

39. (previously presented) The method of claim 36 wherein the networks are Internet Protocol networks.

40. (previously presented) The method of claim 39 wherein the untrusted access station does not assign a global IP address to the terminal but allows the terminal to receive an IP address from the trusted network services.

41. (previously presented): The method of claim 39 wherein the access station assigns the terminal a special IP address acknowledging that it is able to provide access to the trusted network services.

EVIDENCE APPENDIX:

None.

RELATED PROCEEDINGS APPENDIX

None.